ADVANCED COURSE IN ENGINEERING

2004 CYBER SECURITY BOOT CAMP

2Lt David Aparicio
Air Force Research Laboratory
Rome Research Site, Rome, NY
July 21, 2004

Firsthand Testimonial

In his introduction of **The National Strategy to Secure Cyberspace**, President George W. Bush wrote that "securing cyberspace is an extraordinarily difficult strategic challenge that requires coordinated and focused effort from our entire society" and that "the cornerstone of America's cyberspace security strategy is a public-private partnership."

Last summer, I had the distinct privilege of participating in the Advanced Course in Engineering (ACE) on cyber security at the Air Force Research Laboratory Information Directorate (AFRL/IF) in Rome, New York. The program immersed me into ten grueling weeks of research, problem solving and report writing on a variety of cyber security issues. I completed all requirements to call myself an ACE graduate, and I earned the distinction of Class Valedictorian. I gained far more than just a certificate of completion. I gained a mastery of the issues of cyber security which challenge our nation today and shape our future.

ACE uses a unique approach towards running the program. Once a week, students are immersed into one-day lecture covering a specific area in cyber security, concluding with the assignment of a real-world problem. The students must solve the problem and write a report detailing their solution. For the rest of each week, students work with personal mentors on military and industry projects within the Rome Research Site. The week concludes with an 8-mile run. This unique combination of high-intensity instruction, military and industry projects, and an 8-mile run create an environment that develops cyber security leadership and situational awareness vital to our future. ACE taught me not only technical competence but mental flexibility to solve any problem, placed in front of me, academic or critical.

Although my academic background was in electrical engineering, I successfully competed in a program dominated by computer engineers and scientists. I proceeded with great enthusiasm and duty because cyber security is a gravely serious business. ACE introduced me to many of the challenges of the cyber security. Responding to the challenge, I requested to return to the AFRL/IF to contribute to the defense of our Nation through cyber security awareness. I plan to eventually work for the CIA or NSA with my new view of the world.

Many of my fellow ACE graduates received commissions where they put to good use their increased command of cyber security and their appreciation of its impact of national security.

ACE Background

The Advanced Course in Engineering on Cyber Security (ACE) addresses the challenge of the National Strategy to Secure Cyberspace by developing the top students in pre-commissioning officers training programs into the next generation of cyber security leaders. Through a public-private partnership among the Air Force Research Laboratory Information Directorate, Syracuse University, the CASE Center of the New York State Office of Science Technology and Academic Research, the Griffiss Institute on Information Assurance and several corporations, the ACE follows the proven model of the General Electric Edison course to transform engineers into original thinkers, problem solvers and technical leaders.

Far from creating another computer security training program, the ACE seeks to develop cyber security leaders by drawing from the top students in Air Force, Army and Navy pre-commissioning training programs, in addition to the best among our civilian college students. The pedagogical philosophy underlying the ACE seeks to develop leadership skills through intensive formal education, team work and problem solving, mentoring and immersion in a work environment, participation in military leadership activities, and a weekly 8-mile run.

The ACE philosophy is best summarized in the following paradigm: faced with a real-world problem, the graduates of the ACE learn to:

1. formulate a clear problem statement,
2. make reasonable assumptions,
3. apply sound analytical techniques and engineering tools,
4. solve the problem to a certain depth,
5. perform risk analysis on the solution, and
6. deliver a solution on time through effective communication means.

This mindset of an engineering leader was best described by Gene Kranz in his book “Failure is not an Option.” As director of NASA’s mission control in the Apollo era, Kranz led his engineers into uncharted territory, the Moon’s, and established our unchallenged leadership of space.

Cyberspace in the twenty-first century is no less challenging than outer space in the twentieth century. Besides, the security of our Nation relies on establishing and maintaining unchallenged leadership in cyberspace.

In its second year at the Rome Research Site, the ACE has attracted students from 25 colleges in 17 states. In addition to ROTC, the students include fellowship recipients from the National Science Foundation Scholarship for Service Cyber Corps program, cadets from the Air Force Junior ROTC, and civilian scientists and engineers committed to careers in cyber security.

The educators include faculty from Syracuse University, the US Military Academy at West Point and the State University of New York, in addition to domain experts from the Air Force Research Laboratory and industry.

Besides attending formal class work and solving real-world problems, the students spend about three days each week working under the tutelage of a mentor. The mentors include active duty and retired officers at the Air National Guard North East Air Defense Sector, the Air Force Research Laboratory and several local companies.

The duration of the ACE is ten weeks during the June-August timeframe. Each week focuses on one area of cyber security as detailed below:

1. Legal Issues: Internet laws and cyber crime, the Fourth Amendment of the US Constitution, search and seizure of data, rights and privacy issues, government versus private workplace, search warrants and wiretap laws, the Patriot's Act.
2. Security Policies: establishing and implementing security policies, confidentiality integrity and availability considerations, identifying vulnerabilities and threats, establishing disaster response and recovery procedures.
3. Cryptography: mathematical basis for data encryption, substitution ciphers and the Data Encryption Standard, private-key and public-key cryptography, key distribution and trusted authority, digital signatures.
4. Computer Security: operating systems and file system security, passwords and one-way hashes, user-space administration, archiving and back-up strategy, intrusion detection, disaster response and recovery.
5. Digital Forensics: procuring and analyzing digital evidence, preserving the chain of custody of digital evidence, recovering hidden data on hard drives, classifying file systems, analyzing slack and sector data, recovering lost clusters.
6. Network Security: TCP-IP packet format and vulnerabilities, protocol and implementation flaws, buffer overflow, denial-of-service attacks, distributed attacks, email, domain name system, web servers.
7. Network Defense: host and network security, firewalls and periphery intrusion detection systems, bastion hosts, network monitors and traffic analyzers, network logfiles, detecting anomalous behavior, network recovery.
8. Network Attack: port scanners and packet sniffers, IP spoofing, identifying vulnerabilities, designing and implementing network attacks, engineering malicious code, worms and viruses, offensive cyber warfare.
9. Steganography: data hiding in images, classifying steganography algorithms and tools, categorizing vessel capacity, detection and recovery of hidden data, digital watermarking, streaming media steganography, multilingual steganography.
10. Next-Generation Cyber Security: wireless local area networks, wireless encryption protocols, Next-Generation Internet Protocols IPv6, embedded systems, 3G cell phones and personal data assistants.

For each topic, the instructor in charge will assign a substantial real-world problem that requires 40 to 80 hours of team work to solve. Students work on teams of three to solve each problem, then write and submit individual reports.

The military component of the ACE includes:

- residence in converted military barracks at the former Griffiss Air Base
- a weekly run of 8 miles to develop Esprit De Corps and mental toughness
- a staff ride to the Gettysburg battlefield for a lesson in military history
- visits to the North East Air Defense Sector in Rome, the 174th Air Wing in Syracuse, and Phoenix Warrior exercises at Fort Drum.

Recommendations

The federal government can help cyber security in two ways. First, the government should help by increasing efforts to recruit to the younger generations, namely middle and high school students. ACE currently reaches to junior ROTC programs to train college-bound students in cyber security. Secondly, the government should consider increasing its cyber security education through public service announcements. Just as the government shows anti-drug campaign videos on television, basic cyber security videos should be a staple of the American television.

About 2Lt David J. Aparicio

2Lt David Aparicio is a developmental electrical engineer for the Air Force Research Laboratory Information Directorate in Rome, New York. He supports research and development of tools for multi-sensor exploitation and communication intelligence. Lt Aparicio was born in Portland, Oregon but calls Sugar Land, Texas his native home. He earned his bachelor of science in electrical and computer engineering at Baylor University and received his commission as a Blue Chip graduate of Baylor's ROTC program in 2003. Lt Aparicio was also a graduate and the valedictorian of the Advanced Course in Engineer on Cyber Security in 2003. In his free time, Lt Aparicio enjoys photography, writing, and playing soccer.